F .ENT COOPERATION TREA. .

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 29 May 2000 (29.05.00)	
International application No. PCT/DE99/03262	**Applicant's or agent's file reference** GR 98P2998P
International filing date (day/month/year) 11 October 1999 (11.10.99)	**Priority date** (day/month/year) 03 November 1998 (03.11.98)
Applicant EUCHNER, Martin	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

12 April 2000 (12.04.00)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

Maria Kirchner

Telephone No.: (41-22) 338.83.38

09/831046

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference GR 98P2998P	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/DE99/03262	International filing date (*day/month/year*) 11 October 1999 (11.10.99)	Priority date (*day/month/year*) 03 November 1998 (03.11.98)
International Patent Classification (IPC) or national classification and IPC H04L 9/32		
Applicant SIEMENS AKTIENGESELLSCHAFT		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 3 sheets.

RECEIVED
NOV 13 2001
Group 2100

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
12 April 2000 (12.04.00)	09 January 2001 (09.01.2001)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/DE99/03262

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☐ the international application as originally filed.

☒ the description, pages 1-11, as originally filed,
pages _____, filed with the demand,
pages _____, filed with the letter of _____.
pages _____, filed with the letter of _____.

☒ the claims, Nos. _____, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1-8, filed with the letter of 18 December 2000 (18.12.2000),
Nos. _____, filed with the letter of _____.

☒ the drawings, sheets/fig 1/3-3/3, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____.
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: III.

See Box VIII.1 below.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/DE 99/03262

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-7	YES
	Claims		NO
Inventive step (IS)	Claims		YES
	Claims	1-7	NO
Industrial applicability (IA)	Claims	1-7	YES
	Claims		NO

2. Citations and explanations

1. Reference is made to the following document:

D1 = US-A-5 241 599.

2.1 Document D1 is considered to be the closest prior art with respect to the subject matter of Claim 1. It discloses (see Figure 5 and the associated text; the references in parentheses relate to D1) a process for producing secret codes,

a) in which a first instance (Alice) carries out a first operation on predetermined known values (α, β) and a value R_A known only to the first instance, the first operation $(\alpha^{R_A} \bmod \beta)$ being an asymmetrical encryption process;

b) in which the result $(\alpha^{R_A} \bmod \beta)$ of the first operation is encrypted with a first key (P) known to the first instance (Alice) and a first key (P) known to the second instance (Bob), encryption being carried out with the first key using a symmetrical encryption process ("symmetric key cryptosystem");

c) in which the result encrypted with the first key ($P(\alpha^{R_A} \bmod \beta)$) of the first operation is transmitted by the first instance to the second instance;

d) and in which the result of the first operation is decrypted by the second instance with the first key.

The key (P) of the symmetrical encryption process is known only to the two parties participating in the process and the first instance is therefore implicitly authenticated by the second instance by using that key.

2.2 The features (e) and (f) of independent Claim 1 are not disclosed *per se* by D1, and the subject matter of said claim and of dependent Claims 2-7 is thus novel.

2.3 The features mentioned, however, convey no particular advantage and are largely equivalent to the features of the process disclosed in D1, both symmetrical and also asymmetrical encryption being used. Consequently, the subject matter of Claim 1 does not involve an inventive step.

3. The features of dependent Claims 2-7 are either disclosed by the documents cited in the search report or concern measures of common practice in the art that involve no inventive step.

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. Contrary to the requirements of PCT Rule 5.1(a)(ii), the description does not cite document D1 or indicate the relevant prior art disclosed therein.

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1. Claim 8 is too vaguely defined (PCT Article 6); it would be possible to carry out a process according to one of Claims 1-7 in nearly every programmable processor unit with sufficient capacity.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

Absender: INTERNATIONALE RECHERCHENBEHÖRDE

PCT

MITTEILUNG ÜBER DIE ÜBERMITTLUNG DES INTERNATIONALEN RECHERCHENBERICHTS ODER DER ERKLÄRUNG

(Regel 44.1 PCT)

An
SIEMENS AKTIENGESELLSCHAFT
Postfach 22 16 34
D-80506 München
GERMANY

ZT GG VM Mch P/Ri
Eing. 20. März 2000
GR
Frist

Aktenzeichen des Anmelders oder Anwalts GR 98P2998P	Absendedatum *(Tag/Monat/Jahr)* 16/03/2000 **WEITERES VORGEHEN** siehe Punkte 1 und 4 unten
Internationales Aktenzeichen PCT/DE 99/03262	Internationales Anmeldedatum *(Tag/Monat/Jahr)* 11/10/1999
Anmelder SIEMENS AKTIENGESELLSCHAFT et al.	

1. [X] Dem Anmelder wird mitgeteilt, daß der internationale Recherchenbericht erstellt wurde und ihm hiermit übermittelt wird.

Einreichung von Änderungen und einer Erklärung nach Artikel 19:
Der Anmelder kann auf eigenen Wunsch die Ansprüche der internationalen Anmeldung ändern (siehe Regel 46):

Bis wann sind Änderungen einzureichen?

Die Frist zur Einreichung solcher Änderungen beträgt üblicherweise zwei Monate ab der Übermittlung des internationalen Recherchenberichts; weitere Einzelheiten sind den Anmerkungen auf dem Beiblatt zu entnehmen.

Wo sind Änderungen einzureichen?

Unmittelbar beim Internationalen Büro der WIPO, 34, CHEMIN des Colombettes, CH-1211 Genf 20, Telefaxnr.: (41-22) 740.14.35

Nähere Hinweise sind den Anmerkungen auf dem Beiblatt zu entnehmen.

2. [ ] Dem Anmelder wird mitgeteilt, daß kein internationaler Recherchenbericht erstellt wird und daß ihm hiermit die Erklärung nach Artikel 17(2)a) übermittelt wird.

3. [ ] **Hinsichtlich des Widerspruchs** gegen die Entrichtung einer zusätzlichen Gebühr (zusätzlicher Gebühren) nach Regel 40.2 wird dem Anmelder mitgeteilt, daß

[ ] der Widerspruch und die Entscheidung hierüber zusammen mit seinem Antrag auf Übermittlung des Wortlauts sowohl des Widerspruchs als auch der Entscheidung hierüber an die Bestimmungsämter dem Internationalen Büro übermittelt worden sind.

[ ] noch keine Entscheidung über den Widerspruch vorliegt; der Anmelder wird benachrichtigt, sobald eine Entscheidung getroffen wurde.

4. **Weiteres Vorgehen:** Der Anmelder wird auf folgendes aufmerksam gemacht:

Kurz nach Ablauf von **18 Monaten** seit dem Prioritätsdatum wird die internationale Anmeldung vom Internationalen Büro veröffentlicht. Will der Anmelder die Veröffentlichung verhindern oder auf einen späteren Zeitpunkt verschieben, so muß gemäß Regel 90bis.1 bzw. 90bis.3 vor Abschluß der technischen Vorbereitungen für die internationale Veröffentlichung eine Erklärung über die Zurücknahme der internationalen Anmeldung oder des Prioritätsanspruchs beim Internationalen Büro eingehen.

Innerhalb von **19 Monaten** seit dem Prioritätsdatum ist ein Antrag auf internationale vorläufige Prüfung einzureichen, wenn der Anmelder den Eintritt in die nationale Phase bis zu 30 Monaten seit dem Prioritätsdatum (in manchen Ämtern sogar noch länger) verschieben möchte.

Innerhalb von **20 Monaten** seit dem Prioritätsdatum muß der Anmelder die für den Eintritt in die nationale Phase vorgeschriebenen Handlungen vor allen Bestimmungsämtern vornehmen, die nicht innerhalb von 19 Monaten seit dem Prioritätsdatum in der Anmeldung oder einer nachträglichen Auswahlerklärung ausgewählt wurden oder nicht ausgewählt werden konnten, da für sie Kapitel II des Vertrages nicht verbindlich ist.

Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Bevollmächtigter Bediensteter Grace Casuga

(Siehe Anmerkungen auf Beiblatt)

ANMERKUNGEN ZU FORMBLATT PCT/ISA/220

Diese Anmerkungen sollen grundlegende Hinweise zur Einreichung von Änderungen gemäß Artikel 19 geben. Diesen Anmerkungen liegen die Erfordernisse des Vertrags über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens (PCT), der Ausführungsordnung und der Verwaltungsrichtlinien zu diesem Vertrag zugrunde. Bei Abweichungen zwischen diesen Anmerkungen und obengenannten Texten sind letztere maßgebend. Nähere Einzelheiten sind dem PCT-Leitfaden für Anmelder, einer Veröffentlichung der WIPO, zu entnehmen.
Die in diesen Anmerkungen verwendeten Begriffe "Artikel", "Regel" und "Abschnitt" beziehen sich jeweils auf die Bestimmungen des PCT-Vertrags, der PCT-Ausführungsordnung bzw. der PCT-Verwaltungsrichtlinien.

HINWEISE ZU ÄNDERUNGEN GEMÄSS ARTIKEL 19

Nach Erhalt des internationalen Recherchenberichts hat der Anmelder die Möglichkeit, einmal die Ansprüche der internationalen Anmeldung zu ändern. Es ist jedoch zu betonen, daß, da alle Teile der internationalen Anmeldung (Ansprüche, Beschreibung und Zeichnungen) während des internationalen vorläufigen Prüfungsverfahrens geändert werden können, normalerweise keine Notwendigkeit besteht, Änderungen der Ansprüche nach Artikel 19 einzureichen, außer wenn der Anmelder z.B. zum Zwecke eines vorläufigen Schutzes die Veröffentlichung dieser Anspruche wünscht oder ein anderer Grund für eine Änderung der Ansprüche vor ihrer internationalen Veröffentlichung vorliegt. Weiterhin ist zu beachten, daß ein vorläufiger Schutz nur in einigen Staaten erhältlich ist.

Welche Teile der internationalen Anmeldung können geändert werden?

Im Rahmen von Artikel 19 können nur die Ansprüche geändert werden.

In der internationalen Phase können die Ansprüche auch nach Artikel 34 vor der mit der internationalen vorläufigen Prüfung beauftragten Behörde geändert (oder nochmals geändert) werden. Die Beschreibung und die Zeichnungen können nur nach Artikel 34 vor der mit der internationalen vorläufigen Prüfung beauftragten Behörde geändert werden.

Beim Eintritt in die nationale Phase können alle Teile der internationalen Anmeldung nach Artikel 28 oder gegebenenfalls Artikel 41 geändert werden.

Bis wann sind Änderungen einzureichen?

Innerhalb von zwei Monaten ab der Übermittlung des internationalen Recherchenberichts oder innerhalb von sechzehn Monaten ab dem Prioritätsdatum, je nachdem, welche Frist später abläuft. Die Änderungen gelten jedoch als rechtzeitig eingereicht, wenn sie dem Internationalen Büro nach Ablauf der maßgebenden Frist, aber noch vor Abschluß der technischen Vorbereitungen für die internationale Veröffentlichung (Regel 46.1) zugehen.

Wo sind die Änderungen nicht einzureichen?

Die Änderungen können nur beim Internationalen Büro, nicht aber beim Anmeldeamt oder der Internationalen Recherchenbehörde eingereicht werden (Regel 46.2).

Falls ein Antrag auf internationale vorläufige Prüfung eingereicht wurde/wird, siehe unten.

In welcher Form können Änderungen erfolgen?

Eine Änderung kann erfolgen durch Streichung eines oder mehrerer ganzer Ansprüche, durch Hinzufügung eines oder mehrerer neuer Ansprüche oder durch Änderung des Wortlauts eines oder mehrerer Ansprüche in der eingereichten Fassung.

Für jedes Anspruchsblatt, das sich aufgrund einer oder mehrerer Änderungen von dem ursprünglich eingereichten Blatt unterscheidet, ist ein Ersatzblatt einzureichen.

Alle Ansprüche, die auf einem Ersatzblatt erscheinen, sind mit arabischen Ziffern zu numerieren. Wird ein Anspruch gestrichen, so brauchen, die anderen Ansprüche nicht neu numeriert zu werden. Im Fall einer Neunumerierung sind die Ansprüche fortlaufend zu numerieren (Verwaltungsrichtlinien, Abschnitt 205 b)).

Die Änderungen sind in der Sprache abzufassen, in der dieinternationale Anmeldung veröffentlicht wird.

Welche Unterlagen sind den Änderungen beizufügen?

Begleitschreiben (Abschnitt 205 b)):

Die Änderungen sind mit einem Begleitschreiben einzureichen.

Das Begleitschreiben wird nicht zusammen mit der internationalen Anmeldung und den geänderten Ansprüchen veröffentlicht. Es ist nicht zu verwechseln mit der "Erklärung nach Artikel 19(1)" (siehe unten, "Erklärung nach Artikel 19 (1)").

Das Begleitschreiben ist nach Wahl des Anmelders in englischer oder französischer Sprache abzufassen. Bei englischsprachigen internationalen Anmeldungen ist das Begleitschreiben aber ebenfalls in englischer, bei französischsprachigen internationalen Anmeldungen in französischer Sprache abzufassen.

ANMERKUNGEN ZU FORMBLATT PCT/ISA/220 (Fortsetzung)

Im Begleitschreiben sind die Unterschiede zwischen den Ansprüchen in der eingereichten Fassung und den geänderten Ansprüchen anzugeben. So ist insbesondere zu jedem Anspruch in der internationalen Anmeldung anzugeben (gleichlautende Angaben zu verschiedenen Ansprüchen können zusammengefaßt werden), ob

i) der Anspruch unverändert ist;

ii) der Anspruch gestrichen worden ist;

iii) der Anspruch neu ist;

iv) der Anspruch einen oder mehrere Ansprüche in der eingereichten Fassung ersetzt;

v) der Anspruch auf die Teilung eines Anspruchs in der eingereichten Fassung zurückzuführen ist.

Im folgenden sind Beispiele angegeben, wie Änderungen im Begleitschreiben zu erläutern sind:

1. [Wenn anstelle von ursprünglich 48 Ansprüchen nach der Änderung einiger Ansprüche 51 Ansprüche existieren]:
"Die Ansprüche 1 bis 29, 31, 32, 34, 35, 37 bis 48 werden durch geänderte Ansprüche gleicher Numerierung ersetzt; Ansprüche 30, 33 und 36 unverändert; neue Ansprüche 49 bis 51 hinzugefügt."

2. [Wenn anstelle von ursprünglich 15 Ansprüchen nach der Änderung aller Ansprüche 11 Ansprüche existieren]:
"Geänderte Ansprüche 1 bis 11 treten an die Stelle der Ansprüche 1 bis 15."

3. [Wenn ursprünglich 14 Ansprüche existierten und die Änderungen darin bestehen, daß einige Ansprüche gestrichen werden und neue Ansprüche hinzugefügt werden]:
Ansprüche 1 bis 6 und 14 unverändert; Ansprüche 7 bis 13 gestrichen; neue Ansprüche 15, 16 und 17 hinzugefügt."Oder" Ansprüche 7 bis 13 gestrichen; neue Ansprüche 15, 16 und 17 hinzugefügt; alle übrigen Ansprüche unverändert."

4. [Wenn verschiedene Arten von Änderungen durchgeführt werden]:
"Ansprüche 1-10 unverändert; Ansprüche 11 bis 13, 18 und 19 gestrichen; Ansprüche 14, 15 und 16 durch geänderten Anspruch 14 ersetzt; Anspruch 17 in geänderte Ansprüche 15, 16 und 17 unterteilt; neue Ansprüche 20 und 21 hinzugefügt."

"Erklärung nach Artikel 19(1)" (Regel 46.4)

Den Änderungen kann eine Erklärung beigefügt werden, mit der die Änderungen erläutert und ihre Auswirkungen auf die Beschreibung und die Zeichnungen dargelegt werden (die nicht nach Artikel 19 (1) geändert werden können).

Die Erklärung wird zusammen mit der internationalen Anmeldung und den geänderten Ansprüchen veröffentlicht.

Sie ist in der Sprache abzufassen, in der die internationale Anmeldung veröffentlicht wird.

Sie muß kurz gehalten sein und darf, wenn in englischer Sprache abgefaßt oder ins Englische übersetzt, nicht mehr als 500 Wörter umfassen

Die Erklärung ist nicht zu verwechseln mit dem Begleitschreiben, das auf die Unterschiede zwischen den Ansprüchen in der eingereichten Fassung und den geänderten Ansprüchen hinweist, und ersetzt letzteres nicht. Sie ist auf einem gesonderten Blatt einzureichen und in der Überschrift als solche zu kennzeichnen, vorzugsweise mit den Worten "Erklärung nach Artikel 19 (1)".

Die Erklärung darf keine herabsetzenden Äußerungen über den internationalen Recherchenbericht oder die Bedeutung von in dem Bericht angeführten Veröffentlichungen enthalten. Sie darf auf im internationalen Recherchenbericht angeführte Veröffentlichungen, die sich auf einen bestimmten Anspruch beziehen, nur im Zusammenhang mit einer Änderung dieses Anspruchs Bezug nehmen.

Auswirkungen eines bereits gestellten Antrags auf internationale vorläufige Prüfung

Ist zum Zeitpunkt der Einreichung von Änderungen nach Artikel 19 bereits ein Antrag auf internationale vorläufige Prüfung gestellt worden, so sollte der Anmelder in seinem Interesse gleichzeitig mit der Einreichung der Änderungen beim Internationalen Büro auch eine Kopie der Änderungen bei der mit der internationalen vorläufigen Prüfung beauftragen Behörde einreichen (siehe Regel 62.2 a), erster Satz).

Auswirkungen von Änderungen hinsichtlich der Übersetzung der internationalen Anmeldung beim Eintritt in die nationale Phase

Der Anmelder wird darauf hingewiesen, daß bei Eintritt in die nationale Phase möglicherweise anstatt oder zusätzlich zu der Übersetzung der Ansprüche in der eingereichten Fassung eine Übersetzung der nach Artikel 19 geänderten Ansprüche an die bestimmten/ausgewählten Ämter zu übermitteln ist.

Nähere Einzelheiten über die Erfordernisse jedes bestimmten/ausgewählten Amts sind Band II des PCT-Leitfadens für Anmelder zu entnehmen.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
GR 98P2998P			
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)*	
PCT/DE 99/ 03262	11/10/1999	03/11/1998	
Anmelder			
SIEMENS AKTIENGESELLSCHAFT et al.			

Dieser internationale Recherchenbericht wurde von der internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1

   [ ] wie vom Anmelder vorgeschlagen

   [ ] keine der Abb.

   [X] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

Beschreibung

Verfahren und Anordnung zur Authentifikation von einer ersten Instanz und einer zweiten Instanz

Die Erfindung betrifft ein Verfahren und eine Anordnung zur Authentifikation einer ersten Instanz mit einer zweiten Instanz und/oder umgekehrt.

Im Rahmen einer Authentifikation (auch: Authentifizierung) erklärt eine erste Instanz gegenüber einer zweiten Instanz verläßlich, daß sie auch tatsächlich die erste Instanz ist. Entsprechend ist bei der Übermittlung von (vertraulichen) Daten sicherzustellen, von wem diese tatsächlich stammen.

Ein symmetrisches Verschlüsselungsverfahren ist aus [1] bekannt. Bei dem symmetrischen Verschlüsselungsverfahren wird ein Schlüssel sowohl für die Ver- als auch für die Entschlüsselung verwendet. Ein Angreifer, der in den Besitz solch eines Schlüssels kommt, kann einen Klartext (die zu verschlüsselnde Information) in Schlüsseltext und umgekehrt transformieren. Das symmetrische Verschlüsselungsverfahren heißt auch Private-Key-Verfahren oder Verfahren mit geheimem Schlüssel. Ein bekannter Algorithmus zur symmetrischen Verschlüsselung ist der DES-Algorithmus (Data Encryption Standard). Er wurde im Jahre 1974 standardisiert unter ANSI X3.92-1981.

Ein asymmetrisches Verschlüsselungsverfahren ist aus [2] bekannt. Dabei ist einem Teilnehmer nicht ein einzelner, sondern ein Schlüsselsystem aus zwei Schlüsseln zugeordnet: Mit dem einen Schlüssel wird die Abbildung des Klartext in eine transformierte Form bewirkt, der andere Schlüssel ermöglicht die inverse Operation und überführt den transformierten Text in Klartext. Solch ein Verfahren heißt asymmetrisch, weil beide Seiten, die an einer kryptographischen Operation beteiligt sind, verschiedene

Schlüssel (eines Schlüsselsystems) einsetzen. Einer der beiden Schlüssel, z.B. ein Schlüssel p, kann öffentlich bekannt gemacht werden, wenn folgende Eigenschaften erfüllt sind:

- Es ist nicht mit vertretbarem Aufwand möglich, aus dem Schlüssel p einen zur inversen Operation notwendigen geheimen Schlüssel s abzuleiten.
- Selbst wenn Klartext mit dem (öffentlichen) Schlüssel p transformiert wird, ist es nicht möglich, daraus den (geheimen) Schlüssel s abzuleiten.

Aus diesem Grund heißt das asymmetrische Verschlüsselungsverfahren auch mit einem öffentlich bekanntmachbaren Schlüssel p Public-Key-Verfahren.

Grundsätzlich ist es möglich, den geheimen Schlüssel s aus dem öffentlichen Schlüssel p herzuleiten. Dies wird jedoch insbesondere dadurch beliebig aufwendig, daß Algorithmen gewählt werden, die auf Problemen der Komplexitätstheorie beruhen. Man spricht bei diesem Algorithmen auch von sogenannten "one-way-trapdoor"-Funktionen. Ein bekannter Vertreter für ein asymmetrisches Verschlüsselungsverfahren ist das Diffie-Hellman-Verfahren [6]. Dieses Verfahren läßt sich insbesondere zur Schlüsselverteilung (Diffie-Hellman key agreement, exponential key exchange) einsetzen.

Unter dem Begriff Verschlüsselung wird die allgemeine Anwendung eines kryptographischen Verfahrens $V(x,k)$ verstanden, bei dem ein vorgegebener Eingabewert x (auch Klartext genannt) mittels eines Geheimnisses k (Schlüssel) in einen Chiffretext $c := V(x,k)$ überführt wird. Mittels eines inversen Entschlüsselungsverfahrens kann durch Kenntnis von c und k der Klartext x rekonstruiert werden. Unter dem Begriff Verschlüsselung versteht man auch eine sogenannte Einweg-Verschlüsselung mit der Eigenschaft, daß es kein inverses, effizient berechenbares Entschlüsselungsverfahren gibt. Beispiele für solch ein Einweg-Verschlüsselungsverfahren ist

eine kryptographische Einwegfunktion bzw. eine kryptographische Hashfunktionen, beispielsweise der Algorithmus SHA-1, siehe [4].

Nun besteht in der Praxis das Problem, daß sichergestellt sein muß, daß ein öffentlicher Schlüssel, der zur Verifikation einer elektronischen Unterschrift eingesetzt wird, tatsächlich der öffentliche Schlüssel dessen ist, von dem man annimmt, daß er der Urheber der übermittelten Daten ist (Gewährleistung der Authentizität des Urhebers). Somit muß der öffentliche Schlüssel zwar nicht geheimgehalten werden, aber er muß authentisch sein. Es gibt bekannte Mechanismen (siehe [3]), die mit viel Aufwand sicherstellen, daß die Authentizität gewährleistet ist. Ein solcher Mechanismus ist die Einrichtung eines sogenannten Trustcenters, das Vertrauenswürdigkeit genießt und mit dessen Hilfe eine allgemeine Authentizität sichergestellt wird. Die Errichtung eines solchen Trustcenters und die Verteilung der Schlüssel von diesem Trustcenter aus sind jedoch überaus aufwendig. Beispielsweise muß bei der Schlüsselvergabe sichergestellt sein, daß auch wirklich der Adressat und kein potentieller Angreifer den Schlüssel bzw. die Schlüssel erhält. Dementsprechend hoch sich die Kosten für Einrichtung und Betrieb des Trustcenters.

Die **Aufgabe** der Erfindung besteht darin, eine Authentifikation sicherzustellen, wobei kein gesonderter Aufwand für eine Zertifizierungsinstanz oder ein Trustcenter investiert werden muß.

Diese Aufgabe wird gemäß den Merkmalen der unabhängigen Patentansprüche gelöst. Weiterbildungen der Erfindung ergeben sich auch aus den abhängigen Ansprüchen.

Zur Lösung der Aufgabe wird ein Verfahren zur Authentifikation von einer ersten Instanz mit einer zweiten Instanz angegeben, bei dem von der ersten Instanz eine

Operation A(x,g) auf einem (öffentlich) vorgegebenen bekannten Wert g und einem nur der ersten Instanz bekannten Wert x durchgeführt wird. Das Ergebnis der ersten Operation wird mit einem der ersten und der zweiten Instanz bekannten ersten Schlüssel verschlüsselt. Das mittels des ersten Schlüssels verschlüsselte Ergebnis der ersten Operation wird von der ersten Instanz zu der zweiten Instanz übermittelt.

Hierbei ist es besonders vorteilhaft, daß ein symmetrisches Verfahren eingesetzt wird, um eine Authentizität einer Instanz gegenüber einer weiteren Instanz herzustellen. Diese Authentizität wird bewirkt ohne Einrichtung einer gesonderten Zertifizierungsinstanz oder eines Trustcenters.

Eine Ausgestaltung besteht darin, daß die erste Operation A(x,g) ein asymmetrisches Kryptoverfahren ist. Insbesondere kann die erste Operation auf einer beliebigen endlichen und zyklischen Gruppe G durchgeführt werden.

Eine weitere Ausgestaltung besteht darin, daß die erste Operation A(x,g) eine Diffie-Hellman-Funktion $G(g^x)$ ist. Alternativ kann die erste Operation auch eine RSA-Funktion x^g sein.

Eine Weiterbildung besteht darin, daß die Gruppe G eine der folgenden Gruppen ist:

a) eine multiplikative Gruppe F_q^* eines endlichen Körpers F_q, insbesondere mit
   - einer multiplikativen Gruppe Z_p^* der ganzen Zahlen modulo einer vorgegebenen Primzahl p;
   - einer multiplikativen Gruppe F_t^* mit $t = 2^m$ über einem endlichen Körper F_t der Charakteristik 2;
   - einer Gruppe der Einheiten Z_n^* mit n als einer zusammengesetzten ganzen Zahl;

b) eine Gruppe von Punkten auf einer elliptischen Kurve über einem endlichen Körper;

c) eine Jacobivariante einer hyperelliptischen Kurve über einem endlichen Körper.

Eine andere Weiterbildung besteht darin, daß das Ergebnis der ersten Operation ein zweiter Schlüssel ist, mit dem die erste Instanz zur Wahrnehmung eines Dienstes auf der zweiten Instanz autorisiert wird.

Eine zusätzliche Ausgestaltung besteht darin, daß der zweite Schlüssel ein sogenannter "Sessionkey" oder eine an eine Applikation gebundene Berechtigung ist.

Auch ist es eine Weiterbildung, daß der zweite Schlüssel bestimmt wird zu

$$G(g^{xy})$$

indem von der zweiten Instanz eine Operation $G(g^{y})$ mit einer nur ihr bekannten geheimen Zahl y durchgeführt wird. Das Ergebnis dieser zweiten Operation wird mit dem ersten Schlüssel verschlüsselt und an die erste Instanz übermittelt.

Eine zusätzliche Weiterbildung besteht darin, daß zur Generierung des zweiten Schlüssels das Diffie-Hellmann-Verfahren eingesetzt wird.

Eine andere Ausgestaltung besteht darin, daß die Verschlüsselung mit dem ersten Schlüssel anhand einer Einwegfunktion, insbesondere einer kryptographischen Einwegfunktion durchgeführt wird. Eine Einwegfunktion zeichnet sich dadurch aus, daß sie in einer Richtung leicht zu berechnen, ihre Invertierung aber nur mit so großem Aufwand machbar ist, daß diese Möglichkeit in der Praxis vernachlässigt werden kann. Ein Beispiel für solch eine Einwegfunktion ist eine kryptographische Hashfunktion, die aus einer Eingabe A eine Ausgabe B erzeugt. Anhand der Ausgabe B kann nicht auf die Eingabe A rückgeschlossen

werden, selbst wenn der Algorithmus der Hashfunktion bekannt ist.

Auch ist es eine Weiterbildung, daß die Verschlüsselung, die mit dem ersten Schlüssel durchgeführt wird, einem symmetrischen Verschlüsselungsverfahren entspricht.

Schließlich ist es eine Weiterbildung, daß die übermittelten Daten vertrauliche Daten sind.

Weiterhin wird zur Lösung der Aufgabe eine Anordnung zur Authentifikation angegeben, bei der eine Prozessoreinheit vorgesehen ist, die derart eingerichtet ist, daß

a) von einer ersten Instanz eine erste Operation $A(x,g)$ auf einem vorgegebenen bekannten Wert g und einem nur der ersten Instanz bekannten Wert x durchführbar ist;
b) bei dem das Ergebnis der ersten Operation mit einem der ersten und einer zweiten Instanz bekannten ersten Schlüssel verschlüsselbar ist;
c) bei dem das mit dem ersten Schlüssel verschlüsselte Ergebnis der ersten Operation von der ersten Instanz zu der zweiten Instanz übermittelbar ist;
d) bei dem von der zweiten Instanz mit dem ersten Schlüssel das Ergebnis der ersten Operation entschlüsselt wird und somit die erste Instanz authentifizierbar ist.

Diese Anordnung ist insbesondere geeignet zur Durchführung des erfindungsgemäßen Verfahrens oder einer seiner vorstehend erläuterten Weiterbildungen.

Ausführungsbeispiele der Erfindung werden nachfolgend anhand der Zeichnung dargestellt und erläutert.

Es zeigen

Fig.1 eine Skizze zur Vereinbarung eines gemeinsamen Schlüssels zwischen zwei Instanzen, deren jede Authentizität jeweils sichergestellt ist;

Fig.2 eine Skizze gemäß Fig.1 unter Einsatz des DES-Algorithmus;

Fig.3 eine Prozessoreinheit.

In **Fig.1** ist eine Skizze dargestellt zur Vereinbarung eines gemeinsamen Schlüssels zwischen zwei Instanzen, deren jede Authentizität jeweils sichergestellt ist. Eine Instanz A 101 wählt eine zufällige Zahl x in einem Körper "mod p-1" (siehe Block 103). Nun wird von der Instanz 101 an eine Instanz 102 eine Nachricht 104 geschickt, die folgendes Format aufweist:

$$g,\ p,\ T_A,\ ID_A,\ g^x \bmod p,\ H(g^x \bmod p,\ PW,\ ID_A,\ T_A,\ldots),$$

wobei

x	einen geheimen Zufallswert der Instanz A 101,
y	einen geheimen Zufallswert der Instanz B 102,
g	einen Generator nach dem Diffie-Hellman-Verfahren,
p	eine Primzahl für das Diffie-Hellman-Verfahren,
T_A	einen Zeitstempel der Instanz A beim Erzeugen bzw. Absenden der Nachricht,
T_B	einen Zeitstempel der Instanz B beim Erzeugen bzw. Absenden der Nachricht,
ID_A	ein Identifikationsmerkmal der Instanz A,
ID_B	ein Identifikationsmerkmal der Instanz B,
$g^x \bmod p$	ein öffentlicher Diffie-Hellman-Schlüssel der Instanz A,

$g^y \bmod p$	ein öffentlicher Diffie-Hellman-Schlüssel der Instanz B,
PW	ein gemeinsames Geheimnis zwischen den Instanzen A und B (Paßwort, "shared secret"),
H(M)	eine kryptographische Einwegfunktion (Hashfunktion) über die Parameter M,
KEY	ein beiden Instanzen A und B gemeinsamer Sessionkey.

bezeichnen. Ist diese Nachricht bei der Instanz 102 angekommen, wird dort (siehe Block 105) eine zufällige Zahl y aus dem Körper "mod p-1" gewählt und in einem Block 106 ein gemeinsamer Schlüssel vereinbart zu

$$KEY = g^{xy} \bmod p.$$

Die zweite Instanz 102 übermittelt eine Nachricht 107 mit dem Format

$$T_B,\ ID_B,\ g^y \bmod p,\ H(g^y \bmod p,\ PW,\ ID_B,\ T_B,...)$$

an die erste Instanz 101. Die erste Instanz 101 wird daraufhin in einem Schritt 108 die Operation

$$KEY = g^{xy} \bmod p$$

aus, woraus sich ebenfalls der gemeinsame Schlüssel KEY ergibt.

Hierbei sei ausdrücklich angemerkt, daß beispielhaft der Körper "mod p-1" als eine von vielen Möglichkeiten herausgegriffen wurde. Ferner werden die Nachrichten 104 und 107 als jeweils eine Möglichkeit von vielen angesehen. Insbesondere sind die zur Adressierung angeführten Felder innerhalb der Nachrichten abhängig von der Applikation bzw. dem verwendeten Übertragungsprotokoll.

In Fig.1 wird eine kryptographische Einweg-Hashfunktion H verwendet. Ein Beispiel zur Übermittlung einer solchen Einweg-Hashfunktion ist der SHA-1-Algorithmus (vergleiche [4]). Der Einsatz eines symmetrischen Verschlüsselungsverfahrens, z.B. des DES-Algorithmus [5], anstatt der Einweg-Hashfunktion H, wird in **Fig.2** dargestellt. Die Blöcke 101, 102, 103, 105, 106 und 108 sind in Fig.2 identisch zu Fig.1. Die von der ersten Instanz 101 an die zweite Instanz 102 übertragene Nachricht 201 hat das Format

$$g,\ p,\ T_A,\ ID_A,\ g^x \bmod p,\ ENC_{PW}(g^x \bmod p,\ PW,\ ID_A,\ T_A,\ldots),$$

wobei

$ENC_{PW}(M)$ ein symmetrisches Verfahren zur Verschlüsselung des Parameters M mit dem Schlüssel PW

bezeichnet.

In umgekehrter Richtung wird von der Instanz 102 an die Instanz 101 in Fig.2 die Nachricht 202 verschickt, die folgendes Format aufweist:

$$T_B,\ ID_B,\ g^y \bmod p,\ ENC_{PW}(g^y \bmod p,\ PW,\ ID_B,\ T_B,\ldots).$$

Hierbei sei insbesondere vermerkt, daß jeweils eine Nachricht (in Fig.1 die Nachricht 104 bzw. in Fig.2 die Nachricht 201) ausreicht, um die erste Instanz 101 gegenüber der zweiten Instanz 102 zu authentifizieren. Sieht man davon ab, daß sich auch die zweite Instanz 102, beispielsweise ein wahrzunehmender Dienst innerhalb einer Netzwerkverbindung, z.B. dem Internet, authentifizieren muß, so kann es ausreichen, wenn lediglich die erste Instanz 101 sich authentifiziert. Dies ist bereits nach Übertragung der jeweils ersten Nachrichten 104 und 201 gegeben. Wählt sich insbesondere die erste Instanz 101 bei der zweiten Instanz 102 ein, so ist häufig davon auszugehen, daß diese zweite

Instanz 102 auch die richtige Instanz ist. Umgekehrt muß die zweite Instanz 102 davon ausgehen können, daß der Anrufer (die erste Instanz 101) auch der ist, für den er sich ausgibt. Somit ist in dieser Richtung, von der ersten Instanz 101 zur zweiten Instanz 102, die Prüfung der Authentizität wichtig.

In **Fig.3** ist eine Prozessoreinheit PRZE dargestellt. Die Prozessoreinheit PRZE umfaßt einen Prozessor CPU, einen Speicher SPE und eine Input/Output-Schnittstelle IOS, die über ein Interface IFC auf unterschiedliche Art und Weise genutzt wird: Über eine Grafikschnittstelle wird eine Ausgabe auf einem Monitor MON sichtbar und/oder auf einem Drucker PRT ausgegeben. Eine Eingabe erfolgt über eine Maus MAS oder eine Tastatur TAST. Auch verfügt die Prozessoreinheit PRZE über einen Datenbus BUS, der die Verbindung von einem Speicher MEM, dem Prozessor CPU und der Input/Output-Schnittstelle IOS gewährleistet. Weiterhin sind an den Datenbus BUS zusätzliche Komponenten anschließbar, z.B. zusätzlicher Speicher, Datenspeicher (Festplatte) oder Scanner.

Literaturverzeichnis:

[1] Christoph Ruland: Informationssicherheit in Datennetzen, DATACOM-Verlang, Bergheim 1993, ISBN 3-89238-081-3, Seiten 42-46.

[2] Christoph Ruland: Informationssicherheit in Datennetzen, DATACOM-Verlang, Bergheim 1993, ISBN 3-89238-081-3, Seiten 73-85.

[3] Christoph Ruland: Informationssicherheit in Datennetzen, DATACOM-Verlang, Bergheim 1993, ISBN 3-89238-081-3, Seiten 101-117.

[4] NIST, FIPS PUB 180-1: Secure Hash Standard, April 1995; http://csrc.nist.gov/fips/fip180-1.ps

[5] NIST, FIPS PUB 81: DES Modes of Operation, December 1980; http://www.itl.nist.gov/div897/pubs/fip81.htm

[6] A. Menezes, P. v. Oorschot, S. Vanstone: Handbook of Applied Cryptography; CRC Press 1996, ISBN 0-8493-8523-7; chapter 12.6 (pp. 515-524).

Patentansprüche

1. Verfahren zur Authentifikation,
   a) bei dem von einer ersten Instanz eine erste Operation A(x,g) auf einem vorgegebenen bekannten Wert g und einem nur der ersten Instanz bekannten Wert x durchgeführt wird;
   b) bei dem das Ergebnis der ersten Operation mit einem der ersten und einer zweiten Instanz bekannten ersten Schlüssel verschlüsselt wird;
   c) bei dem das mit dem ersten Schlüssel verschlüsselte Ergebnis der ersten Operation von der ersten Instanz zu der zweiten Instanz übermittelt wird;
   d) bei dem von der zweiten Instanz mit dem ersten Schlüssel das Ergebnis der ersten Operation entschlüsselt wird und somit die erste Instanz authentifiziert wird.

2. Verfahren nach Anspruch 1,
   bei dem die erste Operation A(x,g) ein asymmetrisches Kryptoverfahren ist.

3. Verfahren nach Anspruch 1 oder 2,
   bei dem die erste Operation A(g,x)
   a) eine Diffie-Hellman-Funktion $G(g^x)$ ist, wobei G() eine beliebige, endliche zyklische Gruppe G ist;
   b) eine RSA-Funktion x^g ist.

4. Verfahren nach einem der vorhergehenden Ansprüche,
   bei dem die erste Operation auf einer Gruppe G durchgeführt wird, wobei die Gruppe G eine der folgenden Gruppen ist:
   a) eine multiplikative Gruppe F_q^* eines endlichen Körpers F_q, insbesondere mit
      - einer multiplikativen Gruppe Z_p^* der ganzen Zahlen modulo einer vorgegebenen Primzahl p;

- einer multiplikativen Gruppe F_t^* mit $t = 2^m$ über einem endlichen Körper F_t der Charakteristik 2;
- einer Gruppe der Einheiten Z_n^* mit n als einer zusammengesetzten ganzen Zahl;

b) eine Gruppe von Punkten auf einer elliptischen Kurve über einem endlichen Körper;

c) eine Jacobivariante einer hyperelliptischen Kurve über einem endlichen Körper.

5. Verfahren nach einem der vorhergehenden Ansprüche, bei dem das Ergebnis der ersten Operation ein zweiter Schlüssel ist, mit dem die erste Instanz zur Wahrnehmung eines Dienstes auf der zweiten Instanz autorisiert wird.

6. Verfahren nach dem vorhergehenden Anspruch, bei dem der zweite Schlüssel ein Sessionkey oder eine an eine Applikation gebundene Berechtigung ist.

7. Verfahren nach einem der Ansprüche 5 oder 6, bei dem der zweite Schlüssel bestimmt wird zu

$G(g^{xy})$,

indem von der zweiten Instanz eine zweite Operation $G(g^y)$ mit einer nur ihr bekannten geheimen Zahl y durchgeführt, das Ergebnis dieser zweiten Operation mit dem ersten Schlüssel verschlüsselt und an die erste Instanz übermittelt wird.

8. Verfahren nach einem der vorhergehenden Ansprüche, bei dem zur Erzeugung des zweiten Schlüssels das Diffie-Hellman-Verfahren eingesetzt wird.

9. Verfahren nach einem der vorhergehenden Ansprüche, bei dem die Verschlüsselung mit dem ersten Schlüssel anhand einer Einwegfunktion, insbesondere einer kryptographischen Einwegfunktion, durchgeführt wird.

10. Verfahren nach einem der Ansprüche 1 bis 6, bei dem die Verschlüsselung mit dem ersten Schlüssel anhand eines symmetrischen Verschlüsselungsverfahrens durchgeführt wird.

11. Verfahren nach einem der vorhergehenden Ansprüche, bei dem die übermittelten Daten vertrauliche Daten sind.

12. Anordnung zur Authentifikation, bei der eine Prozessoreinheit vorgesehen ist, die derart eingerichtet ist, daß

a) von einer ersten Instanz eine erste Operation $A(x,g)$ auf einem vorgegebenen bekannten Wert g und einem nur der ersten Instanz bekannten Wert x durchführbar ist;

b) bei dem das Ergebnis der ersten Operation mit einem der ersten und einer zweiten Instanz bekannten ersten Schlüssel verschlüsselbar ist;

c) bei dem das mit dem ersten Schlüssel verschlüsselte Ergebnis der ersten Operation von der ersten Instanz zu der zweiten Instanz übermittelbar ist;

d) bei dem von der zweiten Instanz mit dem ersten Schlüssel das Ergebnis der ersten Operation entschlüsselt wird und somit die erste Instanz authentifizierbar ist.

Zusammenfassung

Verfahren und Anordnung zur Authentifikation von einer ersten Instanz und einer zweiten Instanz

Um eine erste Instanz bei einer zweiten Instanz zu authentifizieren, wird mittels eines asymmetrischen Kryptoverfahrens eine erste Zahl erzeugt. Diese erste Zahl wird symmetrisch verschlüsselt und an die zweite Instanz übertragen. Die zweite Instanz überprüft die erste Zahl durch Entschlüsselung der zweiten Zahl und authentifiziert damit die erste Instanz.

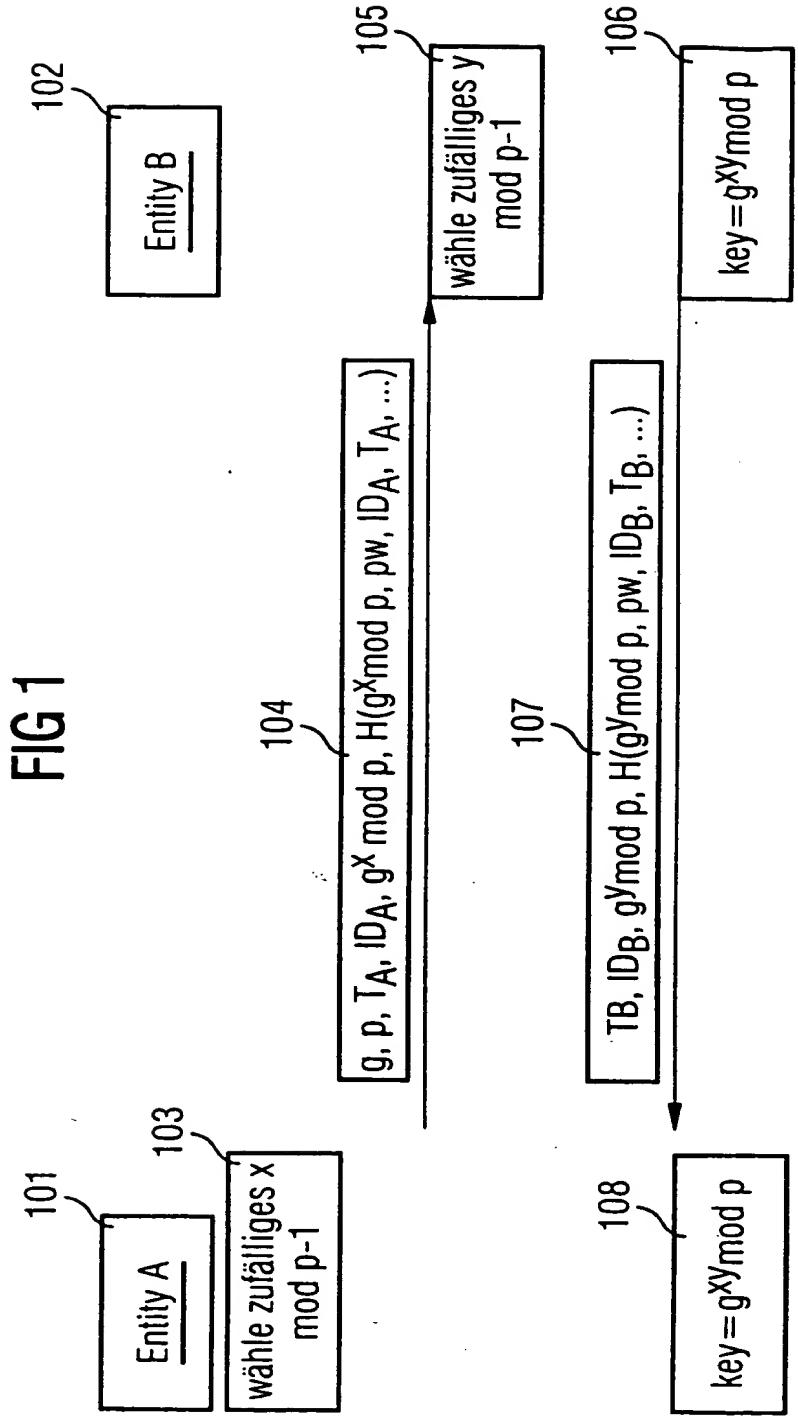

101
Entity A
103
wähle zufälliges x
mod p-1
102
Entity B
105
wähle zufälliges y
mod p-1
106
key=g^XYmod p
104
g, p, T_A, ID_A, g^X mod p, H(g^Xmod p, pw, ID_A, T_A, ...)
107
TB, ID_B, g^Ymod p, H(g^Ymod p, pw, ID_B, T_B, ...)
108
key=g^XYmod p

FIG 1

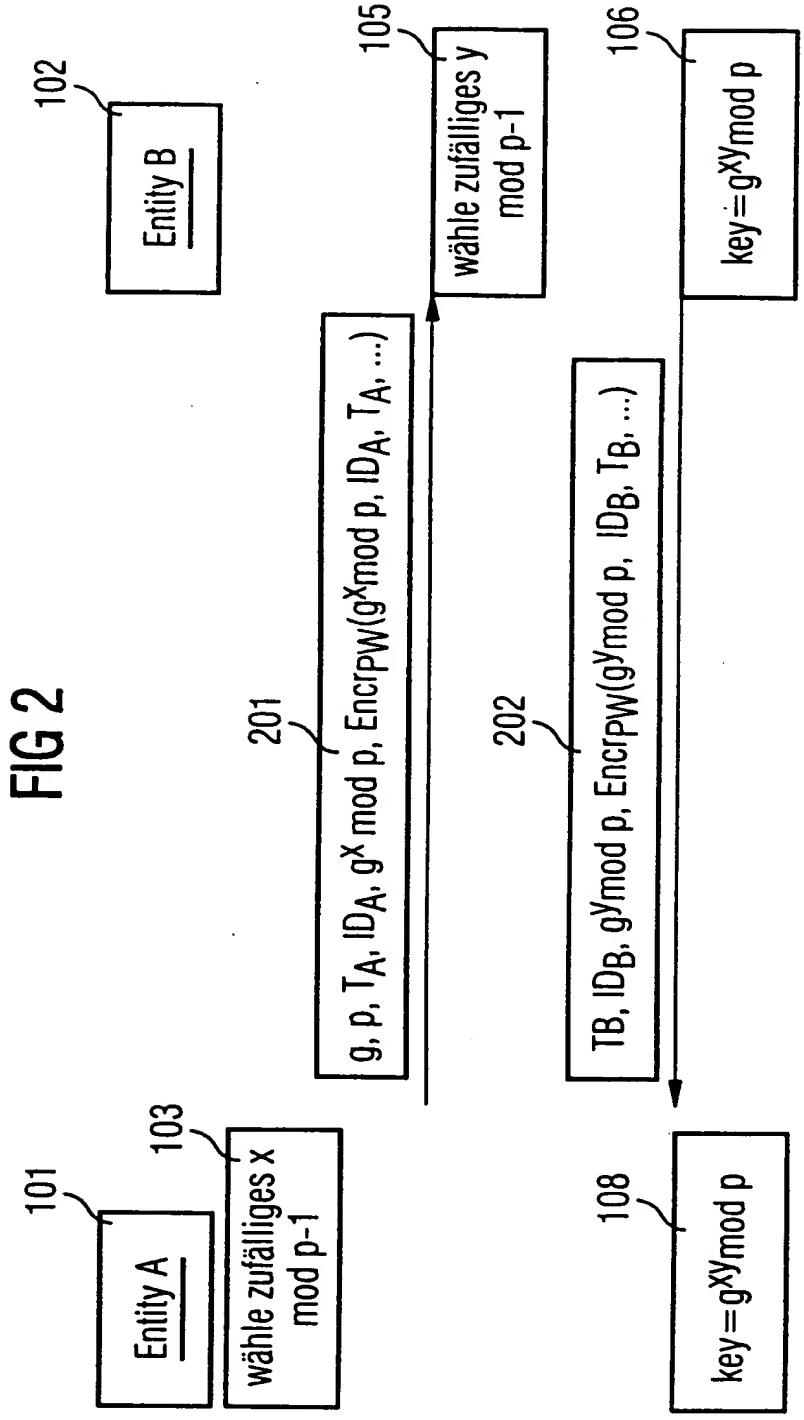
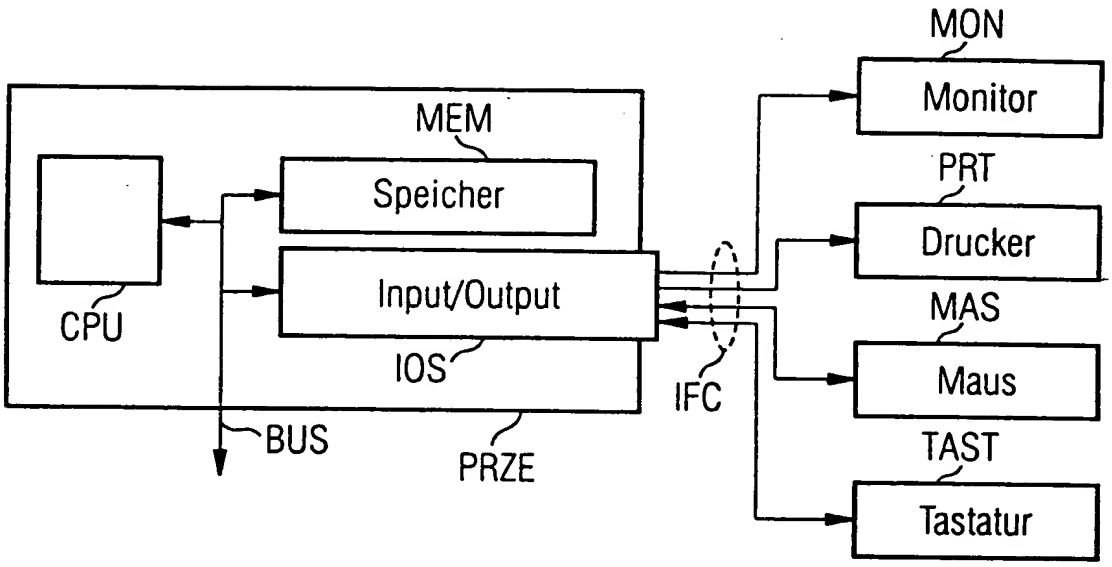

101
Entity A
103
wähle zufälliges x
mod p-1
102
Entity B
105
wähle zufälliges y
mod p-1
106
key=g^xy mod p
201
g, p, T_A, ID_A, g^x mod p, Encr_PW(g^x mod p, ID_A, T_A, ...)
202
TB, ID_B, g^y mod p, Encr_PW(g^y mod p, ID_B, T_B, ...)
108
key=g^xy mod p

FIG 2

FIG 3


MON
Monitor
MEM
Speicher
PRT
Drucker
Input/Output
CPU
MAS
Maus
IOS
IFC
BUS
PRZE
TAST
Tastatur

Patent claims

1. An authenticating method,

a) in which a first entity carries out a first operation A(x,g) on a prescribed known value g and on a value x known only to the first entity;

b) in which the result of the first operation is encoded with the aid of a first key, which is known to the first and to a second entity;

c) in which the result of the first operation encoded with the first key is transmitted by the first entity to the second entity; and

d) in which the result of the first operation is decoded by the second entity with the first key, and the first entity is thereby authenticated.

2. The method as claimed in claim 1, in which the first operation A(x,g) is an asymmetric cryptographic method.

3. The method as claimed in claim 1 or 2, in which the first operation A(g,x)

a) is a Diffie-Hellman function ($G(g^x)$, G() being an arbitrary, finite cyclic group G; and

b) is an RSA function x^g.

4. The method as claimed in one of the preceding claims, in which the first operation is carried out on a group G, the group G being one of the following groups:

a) a multiplicative group F_q^* of a finite body F_q, in particular having

- a multiplicative group Z_p^* of the integers modulo of a prescribed prime number p;

- a multiplicative group F_t^* with $t = 2^m$ over a finite body F_t of characteristic 2;
- a group of units Z_n^* with n as a composite integer;

b) a group of points on an elliptic curve over a finite body; and

c) a Jacobi variant of a hyperelliptic curve over a finite body.

5. The method as claimed in one of the preceding claims, in which the result of the first operation is a second key with which the first entity is authorized to undertake a service on the second entity.

6. The method as claimed in the preceding claim, in which the second key is a session key or an authorization associated with an application.

7. The method as claimed in one of claims 5 or 6, in which the second key is determined in relation to

$G(g^{xy})$,

by virtue of the fact that the second entity carries out a second operation $G(g^y)$ with a secret number y known only to it, encodes the result of this second operation with the first key and transmits it to the first entity.

8. The method as claimed in one of the preceding claims, in which the Diffie-Hellman method is used to generate the second key.

9. The method as claimed in one of the preceding claims, in which the encoding is carried out with the first key with the aid of a one-way function, in particular a cryptographic one-way function.

10. The method as claimed in one of claims 1 to 6, in which the encoding is carried out with the first key with the aid of a symmetrical encoding method.

11. The method as claimed in one of the preceding claims, in which the transmitted data are confidential data.

12. An authenticating arrangement in which a processor unit is provided which is set up in such a way that

a) a first entity can carry out a first operation A(x,g) on a prescribed known value g and on a value x known only to the first entity;

b) the result of the first operation can be encoded with the aid of a first key known to the first and to a second entity;

c) the result of the first operation encoded with the first key can be transmitted by the first entity to the second entity; and

d) the result of the first operation is decoded by the second entity with the first key, and the first entity can thereby be authenticated.

ST

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts	**WEITERES VORGEHEN**	siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)
GR 98P2998P		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Tag)*
PCT/DE99/03262	11/10/1999	03/11/1998
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK		
H04L9/32		
Anmelder		
SIEMENS AKTIENGESELLSCHAFT et al.		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 6 Blätter einschließlich dieses Deckblatts.

   ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt 3 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Berichts
   - II ☐ Priorität
   - III ☒ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☐ Bestimmte angeführte Unterlagen
   - VII ☒ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☒ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
12/04/2000	09.01.2001
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:	Bevollmächtigter Bediensteter
Europäisches Patentamt - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Zucka, G Tel. Nr. +31 70 340 4026

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/DE99/03262

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten.*):
Beschreibung, Seiten:

1-11	ursprüngliche Fassung

Patentansprüche, Nr.:

1-8	eingegangen am	18/12/2000	mit Schreiben vom	18/12/2000

Zeichnungen, Blätter:

1/3-3/3	ursprüngliche Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

   Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

   - ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
   - ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
   - ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

   - ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
   - ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
   - ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
   - ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
   - ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
   - ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

- ☐ Beschreibung, Seiten:
- ☐ Ansprüche, Nr.:
- ☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

   (Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen;sie sind diesem Bericht beizufügen).

6. Etwaige zusätzliche Bemerkungen:

III. Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit

1. Folgende Teile der Anmeldung wurden nicht daraufhin geprüft, ob die beanspruchte Erfindung als neu, auf erfinderischer Tätigkeit beruhend (nicht offensichtlich) und gewerblich anwendbar anzusehen ist:

   ☐ die gesamte internationale Anmeldung.

   ☒ Ansprüche Nr. 8.

Begründung:

☐ Die gesamte internationale Anmeldung, bzw. die obengenannten Ansprüche Nr. beziehen sich auf den nachstehenden Gegenstand, für den keine internationale vorläufige Prüfung durchgeführt werden braucht (*genaue Angaben*):

☒ Die Beschreibung, die Ansprüche oder die Zeichnungen (*machen Sie hierzu nachstehend genaue Angaben*) oder die obengenannten Ansprüche Nr. sind so unklar, daß kein sinnvolles Gutachten erstellt werden konnte (*genaue Angaben*):
siehe Beiblatt

☐ Die Ansprüche bzw. die obengenannten Ansprüche Nr. sind so unzureichend durch die Beschreibung gestützt, daß kein sinnvolles Gutachten erstellt werden konnte.

☐ Für die obengenannten Ansprüche Nr. wurde kein internationaler Recherchenbericht erstellt.

2. Eine sinnvolle internationale vorläufige Prüfung kann nicht durchgeführt werden, weil das Protokoll der Nukleotid- und/oder Aminosäuresequenzen nicht dem in Anlage C der Verwaltungsvorschriften vorgeschriebenen Standard entspricht:

   ☐ Die schriftliche Form wurde nicht eingereicht bzw. entspricht nicht dem Standard.

   ☐ Die computerlesbare Form wurde nicht eingereicht bzw. entspricht nicht dem Standard.

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1-7
	Nein:	Ansprüche	
Erfinderische Tätigkeit (ET)	Ja:	Ansprüche	
	Nein:	Ansprüche	1-7
Gewerbliche Anwendbarkeit (GA)	Ja:	Ansprüche	1-7
	Nein:	Ansprüche	

2. Unterlagen und Erklärungen
siehe Beiblatt

VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:
siehe Beiblatt

VIII. Bestimmte Bemerkungen zur internationalen Anmeldung

Zur Klarheit der Patentansprüche, der Beschreibung und der Zeichnungen oder zu der Frage, ob die Ansprüche in vollem Umfang durch die Beschreibung gestützt werden, ist folgendes zu bemerken:
siehe Beiblatt

Zu Punkt III

Siehe VIII.1 unten.

Zu Punkt V

1. Es wird auf das folgende Dokument verwiesen:

   D1 = US-A-5 241 599

2.1 Das Dokument D1 wird als nächstliegender Stand der Technik gegenüber dem Gegenstand des Anspruchs 1 angesehen. Es offenbart (siehe Figur 5 und dabei hörenden Text; die Verweise in Klammern beziehen sich auf D1) ein Verfahren zur Erzeugung von Geheimschlüsseln,

   a) bei dem von einer ersten Instanz (Alice) eine erste Operation auf vorgegebenen bekannten Werten (α,β) und einem nur der ersten Instanz bekannten Wert R_A durchgeführt wird, wobei die erste Operation (α^{R_A} mod β) ein asymmetrisches Kryptoverfahren ist;

   b) bei dem das Ergebnis (α^{R_A} mod β) der ersten Operation mit einem der ersten (Alice) und einer zweiten (Bob) bekannten ersten Schlüssel (P) verschlüsselt wird, wobei die Verschlüsselung mit dem ersten Schlüssel anhand eines symmetrischen Verschlüsselungsverfahrens ("symmetric key cryptosystem") durchgeführt wird;

   c) bei dem das mit dem ersten Schlüssel verschlüsselte Ergebnis ($P(\alpha^{R_A}$ mod $\beta)$) der ersten Operation von der ersten Instanz zu der zweiten Instanz übermittelt wird;

   d) und bei dem von der zweiten Instanz mit dem ersten Schlüssel das Ergebnis der ersten Operation entschlüsselt wird.

   Der Schlüssel P des symmetrischen Verschlüsselungsverfahrens ist nur den beiden am Verfahren beteiligten Parteien bekannt, und die erste Instanz wird

deshalb durch Benützung dieses Schlüssels implizit bei der zweiten Instanz authentifiziert.

2.2 Die Merkmale (e) und (f) des unabhängigen Anspruchs 1 werden als solche nicht in D1 offenbart, und der Gegenstand dieses Anspruchs, sowie der abhängigen Ansprüche 2-7 ist somit neu.

2.3 Die genannten Merkmale bringen aber keinen besonderen Vorteil, und sind weitgehend gleichwertig zu den Merkmalen des in D1 offenbarten Verfahren, wobei sowohl symmetrische als auch asymmetrische Verschlüsselung verwendet wird. Folglich liegt dem Gegenstand des Anspruchs 1 keine erfinderische Tätigkeit zugrunde.

3. Die Merkmale der abhängigen Ansprüche 2-7 sind entweder von den im Recherchenbericht zitierten Dokumenten offenbart, oder betreffen fachübliche Maßnahmen, an denen keine erfinderische Tätigkeit zugeschrieben werden kann.

Zu Punkt VII

1. Im Widerspruch zu den Erfordernissen der Regel 5.1 a) ii) PCT werden in der Beschreibung weder der im Dokument D1 offenbarte einschlägige Stand der Technik noch dieses Dokument angegeben.

Zu Punkt VIII

1. Der Anspruch 8 ist zu vage definiert (Artikel 6 PCT); in fast jeder programmierbaren Prozessoreinheit mit ausreichender Leistung, wäre ein Verfahren nach einem der Ansprüche 1-7 durchführbar.

Patentansprüche

1. Verfahren zur Authentifikation,
   a) bei dem von einer ersten Instanz eine erste Operation A(x,g) auf einem vorgegebenen bekannten Wert g und einem nur der ersten Instanz bekannten Wert x durchgeführt wird, wobei die erste Operation A(x,g) ein asymmetrisches Kryptoverfahren ist;
   b) bei dem das Ergebnis der ersten Operation mit einem der ersten und einer zweiten Instanz bekannten ersten Schlüssel verschlüsselt wird, wobei die Verschlüsselung mit dem ersten Schlüssel anhand eines symmetrischen Verschlüsselungsverfahrens durchgeführt wird;
   c) bei dem das mit dem ersten Schlüssel verschlüsselte Ergebnis der ersten Operation von der ersten Instanz zu der zweiten Instanz übermittelt wird;
   d) bei dem von der zweiten Instanz mit dem ersten Schlüssel das Ergebnis der ersten Operation entschlüsselt wird und somit die erste Instanz authentifiziert wird;
   e) bei dem das Ergebnis der ersten Operation ein zweiter Schlüssel ist, mit dem die erste Instanz zur Wahrnehmung eines Dienstes auf der zweiten Instanz autorisiert wird;
   f) bei dem der zweite Schlüssel bestimmt wird zu

$$G(g^{xy}),$$

indem von der zweiten Instanz eine zweite Operation $G(g^{y})$ mit einer nur ihr bekannten geheimen Zahl y durchgeführt, das Ergebnis dieser zweiten Operation mit dem ersten Schlüssel verschlüsselt und an die erste Instanz übermittelt wird.

2. Verfahren nach Anspruch 1,
bei dem die erste Operation A(g,x)
a) eine Diffie-Hellman-Funktion $G(g^x)$ ist, wobei G() eine beliebige, endliche zyklische Gruppe G ist oder
b) eine RSA-Funktion x^g ist.

3. Verfahren nach einem der vorhergehenden Ansprüche,
bei dem die erste Operation auf einer Gruppe G durchgeführt wird, wobei die Gruppe G eine der folgenden Gruppen ist:
a) eine multiplikative Gruppe F_q^* eines endlichen Körpers F_q, insbesondere mit
- einer multiplikativen Gruppe Z_p^* der ganzen Zahlen modulo einer vorgegebenen Primzahl p;
- einer multiplikativen Gruppe F_t^* mit $t = 2^m$ über einem endlichen Körper F_t der Charakteristik 2;
- einer Gruppe der Einheiten Z_n^* mit n als einer zusammengesetzten ganzen Zahl;

b) eine Gruppe von Punkten auf einer elliptischen Kurve über einem endlichen Körper;
c) eine Jacobivariante einer hyperelliptischen Kurve über einem endlichen Körper.

4. Verfahren nach dem vorhergehenden Anspruch,
bei dem der zweite Schlüssel ein Sessionkey oder eine an eine Applikation gebundene Berechtigung ist.

5. Verfahren nach einem der vorhergehenden Ansprüche,
bei dem zur Erzeugung des zweiten Schlüssels das Diffie-Hellman-Verfahren eingesetzt wird.

6. Verfahren nach einem der vorhergehenden Ansprüche,
bei dem die Verschlüsselung mit dem ersten Schlüssel anhand einer Einwegfunktion, insbesondere einer kryptographischen Einwegfunktion, durchgeführt wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, bei dem die übermittelten Daten vertrauliche Daten sind.

8. Anordnung zur Authentifikation, bei der eine Prozessoreinheit vorgesehen ist, die derart eingerichtet ist, daß ein Verfahren nach einem der vorhergehenden Ansprüche durchführbar ist.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts GR 98P2998P	WEITERES VORGEHEN	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
Internationales Aktenzeichen PCT/DE 99/ 03262	Internationales Anmeldedatum *(Tag/Monat/Jahr)* 11/10/1999	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)* 03/11/1998
Anmelder SIEMENS AKTIENGESELLSCHAFT et al.		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1

   [ ] wie vom Anmelder vorgeschlagen [ ] keine der Abb.

   [X] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.